C. Amendments to the Claims

1. (Currently Amended) A network storage architecture supporting securely controlled access and bidirectional transfer of data between a client computer system and a network data store, said network storage architecture comprising:

a) an agent program~~,~~ executed on a client computer system and ~~,~~ operative with respect to an application program~~, executable by said client computer system to access a network data store,~~ to develop authentication data with respect to said application program, wherein said application program, as executed by said client computer system, is operative to perform a non-sequential request for the transfer of a first predetermined sub-portion of a predetermined file stored by a network data store, said authentication data including a representation of said non-sequential request; and

b) a network appliance, coupleable through a communications network to said client computer system, interoperable with said agent program to receive and validate said authentication data, said network appliance determining selectively ~~providing a response message to said agent program~~ to control execution of said application program with respect to the performance of said non-sequential request by enabling encrypted transfer of a second predetermined sub-portion of said predetermined file, inclusive of said first predetermined sub-portion, with respect to said network data store.

2. (Currently Amended) The network storage architecture of Claim 1 wherein said authentication data includes user and user session data.

3. (Original) The network storage architecture of Claim 2 wherein said authentication data includes a secure signature of said application program.

4. (Original) The network storage architecture of Claim 1 wherein said agent program is operative to obtain user authentication and collect data with respect to user sessions and processes to develop said authentication data.

5. (Original) The network storage architecture of Claim 4 wherein said agent program is further operative to generate a secure signature of said application program and provide said secure signature as part of said authentication data.

6. (Original) The network storage architecture of Claim 1 wherein said network appliance includes a policy parser operative to evaluate said authentication data and a policy data store including predetermined policy data accessible by said policy parser.

7. (Original) The network storage architecture of Claim 6 wherein said predetermined policy data, as evaluated by said policy parser, is determinative of said response message.

8. (Currently Amended) A network storage architecture supporting securely controlled access and <u>bidirectional</u> transfer of data between a client computer system and a network data store, said network storage architecture comprising:

a) an agent program, executed on a client computer system, responsive to a source file request issued with respect to a network data store by an application program executed by said client computer system, <u>wherein a source file is stored by said network data store and wherein said source file request is a random read/write request specifying transfer of a first defined sub-portion of said source file,</u> said agent program being operative to develop authentication data with respect to said application program and to provide a file request message including a representation of said source file request and said authentication data; and

b) a network appliance, coupleable through a communications network to said client computer system and responsive to said file request message, said network appliance including a policy parser operative to evaluate said file request message and a policy data store including predetermined policy data accessible by said policy parser, said network appliance, responsive to the evaluation of said file request message, enabling performance of said source file request with respect to said network data store <u>including transfer from said network data store</u>

a second defined sub-portion of said source file inclusive of said first defined sub-portion of said source file.

9. (Original) The network storage architecture of Claim 8 wherein said authentication data includes an authenticated identification of a user associated with said application program.

10. (Original) The network storage architecture of Claim 9 wherein said authentication data includes user session and context data.

11. (Original) The network storage architecture of Claim 10 wherein said authentication data includes a secure signature of said application program.

12. (Currently Amended) The network storage architecture of Claim 8 wherein said network appliance enables ~~the~~ generation of a modified file request corresponding to said source file request and directed to said network data store, said modified file request specifying transfer of said second defined sub-portion of said source file.

13. (Original) The network storage architecture of Claim 12 further comprising a first communications network through which said file request message is received by said network appliance and a second communications network through which said modified file request is provided to said network data store.

14. (Currently Amended) The network storage architecture of Claim 13 wherein said network appliance includes an encryption unit and wherein said network appliance further provides for the cipher processing of said second defined sub-portion of said source file as ~~file data~~ transferred in connection with said modified file request such that said first sub-portion of said source file is encrypted as transferred to said network data store.

15. (Original) The network storage architecture of Claim 14 wherein said policy data store further provides for the storage of an encryption key identifier

determinable by said policy parser on evaluation of said file request message and wherein said network appliance obtains an encryption key identified by said encryption key identifier for use in the cipher processing of file data transferred in connection with said modified file request.

16. (Original) The network storage architecture of Claim 15 wherein said authentication data includes a process identifier, corresponding to said application program as executed on said client computer system, a verified user identifier, and a group identifier, and wherein said policy parser is operative to qualify said file request message against said predetermined policy data with respect to said process identifier, verified user identifier, and group identifier.

17. (Currently Amended) A method of securing access by a client computer system to file data stored on a storage device accessible by said client computer system, said method comprising the steps of:

a) intercepting, by a first program as executed on a client computer system, a data transfer request issued by a second program, as executed on said client computer system, directed to a data file stored by a client accessible file data store<u>, wherein said data transfer request specifies transfer of a first sub-portion of said data file to said client accessible file data store</u>;

b) first processing, by said first program, said data transfer request to associate authentication data with said data transfer request;

c) evaluating, by a security appliance coupled to said client computer system through a communications network, said data transfer request, said authentication data, and access control data corresponding to said data file to qualify said data transfer request; and

d) second processing to selectively enable said data transfer request to proceed relative to said data file dependent on the qualification of said data transfer request<u>, said second processing including the steps of</u>

<u>I) retrieving a second sub-portion of said data file;</u>

<u>ii) decrypting said second sub-portion;</u>

<u>iii) incorporating said first sub-portion into said second sub-portion;</u>

<u>iv) encrypting said second sub-portion; and</u>

v) transferring said second sub-portion to said client accessible file data store for incorporation into said data file.

18. (Currently Amended) The method of Claim 17 wherein said authentication data includes process and user context identification information.

19. (Original) The method of Claim 17 wherein said authentication data includes a verified user identifier and a process identifier.

20. (Original) The method of Claim 17 wherein said authentication data includes a verified user identifier, a process identifier, a group identifier.

21. (Currently Amended) The method of Claim 17 wherein said data file includes file data that, as stored by said client accessible file data store, is stored as a plurality of discretely encrypted blocks, wherein said first and second sub-portions of said data file are respectively first and second sub-portions of the file data of said data file, wherein said data transfer request specifies a data range of file data and wherein said second processing step includes the step of modifying said data range to correspond to a sub-plurality of said discretely encrypted blocks defining said second sub-portion, thereby accommodating the ~~accommodate~~ block encryption of file data within said data file.

22. (Original) The method of Claim 17 wherein said step of evaluating associates encryption control data with said data transfer request and wherein said second processing step, responsive to said encryption control data, includes cipher processing of file data transferred in connection with said data transfer request.

23. (Original) The method of Claim 22 further comprising the steps of:

a) first transferring said data transfer request to said security appliance through a first communications network; and

b) second transferring said data transfer request relative to said client accessible file data store through a second communications network.

24. (Original) The method of Claim 23 wherein, through said first and second transferring steps, said security appliance is established a network portal through which network file accesses are routed between said client computer system and said client accessible file data store.

25. (Currently Amended) A method of securing bidirectional file access operations by a client computer system made with respect to a client accessible file data store, said method comprising the steps of:

a) intercepting, by a first program executing on a client computer system, file operation requests issued by a second program, as executing on said client computer system, wherein said file operation requests are issued with respect to files selectively stored encrypted in a filesystem accessible by said client computer system;

b) determining, by said first program relative to a predetermined file operation request, authentication data for said second program, wherein said authentication data includes user and process identification data and a representation of said predetermined file operation request; ~~and~~

c) enabling, by a security appliance responsive to said authentication data, said predetermined file operation request with respect to a file identified by said predetermined file operation request, wherein said enabling step is dependent on qualification, by said security appliance, of said authentication data against policy data defining operation permissions relative to said file including a write operation permission to allow modification of said file as stored encrypted in said filesystem; and

d) transferring predetermined encrypted blocks of file data representing a sub-portion of said file in response to said predetermined file operation request through a network connection where said predetermined encrypted blocks of file data are decrypted, modified, encrypted, and returned through said network connection for storage as part of said file.

26. (Currently Amended) The method of Claim 25 further comprising the steps of:

a) associating an encryption key with said predetermined file operation request determined from the qualification of said authentication data against said policy data; and

b) cipher processing, using said encryption key, said predetermined encrypted blocks of file data transferred relative to said file.

27. (Currently Amended) The method of Claim 26 wherein said predetermined file operation includes a specification of file data to be transferred and wherein said step of cipher processing includes modifying said ~~the~~ specification of said predetermined file operation request to correspond to said predetermined encrypted blocks ~~accommodate encryption~~ of file data transferred relative to said file.

28. (Original) The method of Claim 27 wherein said step of cipher processing is performed on said security appliance.

29. (Original) The method of Claim 28 wherein said authentication data includes a verified user identification and a login process identification.

30. (Currently Amended) A security appliance for securing bidirectional access by client computer systems to persistently stored remotely encrypted data files, said security appliance comprising:

a) a processor coupleable to a client computer system to receive an access request message, wherein said access request message includes authentication data and an identification of a random read/write file data transfer operation directed to an identified data file stored encrypted in a persistent data file store; and

b) a policy data store, accessible by said processor, providing for the storage of predetermined file operation qualifiers applicable to data files present in said persistent data file store, wherein said policy data store is maintained secure by said processor with respect to said client computer system, and wherein

said processor is operative to selectively enable said random read/write file data transfer operation, dependent on an evaluation of said predetermined file operation qualifiers with respect to said access request message to transfer an encrypted sub-portion of said identified data file through a network connection for remote decryption, modification and return through said network connection for storage as part of said identified data file.

31. (Original) The security appliance of Claim 30 wherein said authentication data includes a verified user identifier and a group identifier and wherein said processor is operative to discriminate said verified user identifiers, said group identifier, said file operation and said identified data file against said predetermined file operation qualifiers to obtain said evaluation.

32. (Original) The security appliance of Claim 31 wherein said policy data store further provides for the storage of encryption keys in association with said predetermined file operation qualifiers and wherein said processor is operative to retrieve a predetermined encryption key from said policy data store dependent on said evaluation.

33. (Currently Amended) The security appliance of Claim 32 wherein said processor, responsive to said evaluation, is further operative to provide for said file operation to be passed through said network connection to said persistent data file store.

34. (Currently Amended) The security appliance of Claim 33 wherein said processor, responsive to said evaluation, is further operative to modify a specification of said random read/write file data transfer operation to encompass ~~accommodate~~ the transfer of said encrypted sub-portion of said identified data file ~~encrypted data in connection with the~~ performance of said random read/write file data transfer operation with respect to said identified data file.

35. (Currently Amended) The security appliance of Claim 34 wherein said processor includes an encryption engine operative to process said encrypted sub-portion of said identified data file as ~~encrypted data~~ transferred through said network connection ~~with respect to said identified data file~~.

D. Amendments to the Drawings

Drawing figure 12B has been amended to change the first occurrence of the reference numeral 386 (upper right) to read 366.